13.2.4.1 Accessing Emails of Absent Employees

Access to employee emails should only be undertaken if the employee is away on extended leave and timeframes for meeting the request will not be met. Once it is identified that access will be required to an absent employee's emails, the OPI (not ATIP Division) must coordinate with HQ Infrastructure and Information Security Division (CBSA-ASFC_Network_Monitoring-Surveillance_du_réseau) to obtain access to the emails.

If it is discovered that, for email requests (ie - any and all emails from Jane Doe about John Smith – employee to employee requests), an employee is absent for 2 weeks or more, the Analyst can go back to the requester to advise that the person in question is away from the office. However, we cannot disclose why they are away from the office. Analysts are also to verify with outlook to confirm the out of office of the person, and let the requester decide whether to have someone else process the request or to put it on hold while the person is away. They may even abandon the request entirely. Ensure that any actions are noted in APCM retrieval action.

Should the requester wish to proceed with their request in the employee's absence, the OPI Director or higher must approve the access. The approval (email or otherwise) must include the following elements:

- The ATIP file number and retrieval email;
- Confirmation that the employee is absent during the retrieval period;
- Identification of the individual (the delegate) who should receive access and will be responsible to review the records for release concerns *(if the request pertains to or contains personal information about an employee, that employee must not receive access to the absent employees information or be responsible for the review).*

Security will then set up a drop box and send it to the delegate, and cc the absent employee and advise which key words and criteria were used to conduct the search. Once the review is completed, the package is signed off by the Director or higher and forwarded to the ATIP Liaison for sending to ATIP Division. All emails must be deleted by the delegate. The delegate is to ensure confidentiality of all emails reviewed. The Director is advised to look at key words and decide if the scope is met. If they are unsure, the Director should discuss with the employee upon their return to ensure that all records were retrieved and forward any additional records that were missed (if any exist).

Canada Border Services Agency

Policy on the Overt Use of Audio-Video Monitoring and Recording Technology

Programs Branch
November 2013

Table of Contents

Policy Statement

1. It is the policy of the Canada Border Services Agency (CBSA) to use audio-video monitoring and recording technology in support of its programs, its operations, and for the protection of its employees and assets, while respecting the laws of Canada and the privacy rights of individuals and employees.

2. This policy has been updated to provide guidance on the use of audio-capable equipment and the acceptable locations of such equipment.

3. Future revisions will be made to the policy as the CBSA continues to refine the potential uses of this technology.

Definitions

4. **Administrative Purpose** – as defined in section 3 of the *Privacy Act* - means in respect of personal information about an individual, the use of that information in a decision making process that directly affects that individual.

5. **Audio Capable Cameras** (cameras with microphones) – cameras that can transmit audio without the installation or modification of hardware. This includes cameras that contain a built-in microphone or where there is a connected external microphone.

   a) **Audio-Activated** (microphone activated) – cameras where an operator can listen to live or recorded audio. (Note: This does not currently exist outside of interview rooms)

   b) **Audio-Deactivated** (microphone deactivated) – cameras where an operator cannot listen to live or recorded audio. This includes restricting audio capability in camera firmware or restricting audio capability in the video management system.

6. **Audio-Video Monitoring and Recording Technology** – means any device, recording medium and related technology that can be used by itself or as a unit to view and/or record images, and, in some cases, to hear and/or record sound.

7. **Camera** – means any device used to view or record light or thermal images, with or without audio.

8. **Direct or principal control/use** – means, in reference to third party equipment (see paragraph 20), that although the CBSA does not own the equipment, it maintains the control and use of cameras, as well as access to the recording system, whether or not the third party owner also maintains access to the cameras or recording system.

9. **Employees** – means all persons employed by the CBSA, including uniformed and non-uniformed staff.

10. **Event** – means any occurrence that may reasonably be expected to require further action by the CBSA in support to its legislation, mandate and relevant policies associated with programs delivery.

11. **Monitor** – means to watch, and in the context of this policy, is further defined as watching a screen connected to camera or cameras for the purpose of viewing and/or supervising CBSA operations live, in real-time.

12. **Non-Audio Capable Cameras** (Cameras without microphones) – cameras which cannot transmit audio without the installation or modification of hardware.

    a) **Audio-upgradeable** (microphone-upgradeable) – cameras with audio jack.

    b) **Non Audio-upgradeable** (non-microphone-upgradeable) – camera without audio jack.

13. **Operational Records** – as defined by Library and Archives Canada; are records created, collected or received by a federal government institution to support and document business functions, programs, processes, transactions, services and all other activities uniquely or specifically assigned to that particular institution by legislation, regulation or policy. (Source: MIDA 3, Common Administrative Records, Appendix I - Terms and Conditions, A. Key Definitions)

14. **Overt Monitoring and recording** – refers to the use of cameras and recording devices which are plainly and clearly announced and/or are visible in their placement or use.

15. **Personal information** – as defined in Section 3 of the *Privacy Act* - means information about an identifiable individual that is recorded in any form.

    Note: According to the *Privacy Act*, information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of that individual is <u>not</u> included in this definition.

16. **Port of Entry and CBSA inland service locations** – have the same meanings as in the definition of "customs office" in section 2 of the *Customs Act* and of "port of entry" in section 2 of the *Immigration and Refugee Protection Regulations.*

17. **Public** – means travellers and persons who enter any area used for the purpose of processing persons and/or goods by the CBSA.

18. **Record** – has the same meaning(s) as in section 2 of the *Customs Act* and in section 2 of *National Archives of Canada Act* and, for the purposes of this policy, means any material on which audio-video data is recorded or marked and which is capable of being read or understood by a person, a computer system or other device, regardless of medium or form.

19. **Recording** – means video data, with or without audio, which is being or has been captured in a record and which may be viewed at any time following its creation, until the time of its disposal.

20. **Third party equipment** – means camera and recording equipment that is owned by an entity other than the CBSA.

21. **Transitory Record** – as defined by Library and Archives Canada and for the purposes of this policy are those audio-video records that have no enduring value to the CBSA. They are records that are required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record but **do not** include records that are required to control, support or document the delivery of programs, to carry out operations, to make decisions, or to account for activities of government. (Source: *MIDA 2.1*, 4. Definition)

Authorities

Canada Border Services Agency Act

22. Paragraph 5(1)(a) – states that the CBSA is responsible for providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods, including animals and plants, that meet all requirements under the program legislation by supporting the administration or enforcement, or both, as the case may be, of the program legislation.

Customs Act

23. Subsection 107(1) – defines "customs information" as information of any kind and in any form that relates to one or more persons obtained by or on behalf of the Minister for the purposes of the *Customs Act* or the *Customs Tariff*, or that is prepared from such information.

24. Subsection 107(2) prohibits the release of, unauthorized access to, or the use of any customs information except as permitted under section 107. Section 107 also specifies terms and conditions under which customs information may be disclosed, accessed or used.

Library and Archives of Canada Act

25. Section 9 – authorizes the Librarian and Archivist to dispose of or destroy any publication or record under his or her control, if he or she considers that it is no longer necessary to retain it.

26. Section 12 – prohibits the disposal or destruction of government or ministerial records without the written consent of the Librarian and Archivist or of a person delegated by the Librarian and Archivist to give such consent.

Privacy Act

27. General – the *Privacy Act* requires federal government institutions to respect the privacy rights of individuals by placing limits on the collection, use and disclosure of personal information.

28. Section 3 – defines "personal information" as any information about an identifiable individual that is recorded in any form.

29. Section 4 – states that personal information may not be collected by a government institution unless it relates directly to an operating program or activity of the institution.

30. Sections 7 and 8 – provide that a government institution will not use or disclose personal information without the consent of the individual to whom it relates except under the specific circumstances listed in section 8.

Background

31. Over the past several decades, the CBSA has increasingly implemented the use of audio-video technology to carry out its mandate and to ensure the protection of its assets and staff. The use of closed-circuit television cameras to monitor facilities and operations are now an integral part of the CBSA's security framework and operations management.

32. When the CBSA collects personal information, it has certain obligations regarding the protection of such information. While storing it, the CBSA must ensure that personal information is used only for the purposes for which it was collected or purposes that are authorized by law and that the personal information is only accessed by persons with the need to access it as part of their official duties. Finally, when the information is no longer needed or has served its purpose, it needs to be properly disposed of.

Purpose and Scope

33. The purpose of this policy is to communicate the CBSA's position on the use of overt audio-video monitoring and recording technology at ports of entry and inland service locations and the retention requirements for recordings made using such technology.

34. This policy also sets out who may access such equipment, make copies of, or disclose recordings.

35. This policy applies to all overt audio-video monitoring and recording equipment that is owned or leased by the CBSA, as well as to third party equipment that is directly or principally controlled or used by the CBSA at ports of entry and inland service

locations in support of CBSA's mandate while ensuring compliance with Privacy requirements.

36. This policy applies equally to monitoring and recording equipment that is capable of capturing either audio-video or video-only footage.

37. This policy applies to employees of the CBSA and to any other person who may be authorized to install, operate or maintain equipment, or to view/hear recordings.

38. This policy does not apply to third party audio-video monitoring and recording equipment for which the CBSA does not have direct or principal control or use.

39. This policy does not apply to CBSA employees stationed abroad.

40. This policy does not apply to any circumstance where covert audio-video surveillance may be used and does not supersede any guidelines that have been established by the Courts for the taking of witness or accused statements or interviewing of subjects of a criminal investigation.

41. This policy does not apply to the collection of any non-personal information related solely to the research, design, development or testing of audio or video equipment or technology.

Policy Statements

Permitted Uses

42. The CBSA uses audio-video monitoring and recording technology for the following purposes:

    (a) To carry out the mandate of the CBSA to ensure the integrity of the border in relation to the national security and/or public safety of Canada and its citizens:

    At Ports of Entry

    (i) To detect and identify persons who fail to present themselves and their goods in accordance with sections 11 and/or 12 of the *Customs Act* and/or section 18 of the *Immigration and Refugee Protection Act* ;
    (ii) To detect or deter persons who may pose a risk to the health and safety of CBSA employees and members of the public;
    (iii) To gather information regarding unlawful activity related to any of the legislation enforced by the CBSA (e.g. evidence that goods have been unlawfully removed from CBSA control;

    At Inland CBSA Service Locations

(iv) To detect or deter persons who may pose a risk to the health and safety of CBSA employees and members of the public;
(v) To gather information regarding unlawful activity related to any of the legislation enforced by the CBSA (e.g. evidence that goods have been unlawfully removed from CBSA control);

(b) For the security and protection of CBSA infrastructure including buildings, assets and equipment:

At all Ports of Entry and Inland CBSA Service Locations

(i) To monitor or control access to CBSA owned or operated buildings, assets and equipment to ensure that only those persons requiring or having permission to access buildings, assets and equipment do so;
(ii) To enable an appropriate response to unlawful or unauthorized access to CBSA owned or operated buildings, assets and equipment, including the identification and investigation of persons involved in such activity;

(c) For the security and protection or the health and safety of CBSA employees and/or members of the public working in or having access to CBSA owned or operated facilities including ports of entry or any other CBSA office:

At all Ports of Entry and Inland CBSA Service Locations

(i) To monitor public and other areas where employees of the CBSA work and interact with members of the public to identify, prevent or respond to real or potential threats to the safety CBSA employees or members of the public;
(ii) To monitor open and restricted areas where members of the public have access, or are housed, to identify and respond to medical emergencies, real or potential threats or assaults, or any other health or safety issues involving those individuals and/or CBSA employees.

(d) To ensure the integrity and quality assurance of CBSA programs at all CBSA locations.

43. Managers are permitted to use Audio-Video information live, in real-time, to manage the CBSA operations in the delivery of its programs.

44. If ongoing or repeated breaches of the Code of Conduct are suspected, but **no formal** allegations have been made, an employee's direct supervisor is permitted to use the audio-video equipment **live, in real time**, to confirm or negate those suspicions. Managers are not permitted to review any recordings for this purpose.

45. If recordings are to be used to further an investigation/fact-finding into formal allegations of breaches of the Code of Conduct or illegal activity by a CBSA employee, approval for the use of the recording must be received in writing from the Departmental Security Officer (Security and Professional Standards Directorate). In situations where disciplinary action may be taken, Regional Human Resources Director, Director of Labour Relations and Director, Personnel Security and Professional Standards Division should be consulted.

46. Following an investigation into breaches of the Code of Conduct or illegal activity, related recordings may be used as evidence with the approval of the Director who is responsible for the location where the incident(s) occurred. Approval may also be granted by a Director at another location or the Regional Director General if necessary.

Capture of Audio Information

47. The CBSA will only capture audio information in a manner that respects individual privacy rights protected under the *Canadian Charter of Rights and Freedoms* and the limitations provided for in the *Privacy Act* and the *Criminal Code*.

48. To ensure compliance with this legislation, the CBSA will only capture audio insofar as it relates directly to the mandate of the Agency. This may include interactions between CBSA employees and members of the public but does not include private conversations between individuals.

49. The CBSA currently permits audio capture in interview rooms following full disclosure of the intent to record.

50. The CBSA is exploring the future use of audio capture in the following areas where CBSA employees interact with the public: primary inspection lines (PIL), secondary inspection areas and cash/service counters. (Note: audio capture in these areas must remain de-activated until further notice.)

51. Audio capture where CBSA employees interact with the public at primary inspection lines (PIL), secondary inspection areas and cash/services counters must remain deactivated through usage of video management system

    a. Where technology permits, system access to administration roles shall be limited users based and password protected;
    b. Where technology does not include users based role, access to system administration roles shall be restricted to restricted individuals;

52. The CBSA shall conduct ongoing monitoring and audit of the audio functionality to ensure compliance privacy requirements

Limitations on Use

53. Audio-video **recordings** must not be used to support formal evaluation of individual employee performance.

54. The audio-video monitoring and recording technology shall not be used to monitor any area or activity outside of the CBSA's area of operation.

55. Audio-video monitoring and recording technology shall not be used to monitor any public or employee washroom, nor any lunch or change room.

56. Data collected from audio-video monitoring and recording technology shall not be used for any purpose other than those expressly identified in paragraphs 42 - 52.

57. In accordance with subsection 163.5(4) of the *Customs Act,* audio-video equipment cannot be used for the sole purpose of monitoring for Criminal Code offences.

Capture of Audio Information

58. The audio-capability of cameras located outside of interview rooms must remain deactivated until further notice.

59. The audio-capability of cameras located outside of areas where the CBSA interacts directly with the public in the discharge of its mandate must be disconnected, disabled or removed so that it meets the definition of non-audio capable cameras. For greater clarity this includes all audio-capable cameras outside of primary inspection lines (PIL), secondary areas, cash/service counters and interview rooms.

60. Even within these areas, any audio-capable cameras must be positioned to limit capture to interactions between the CBSA and the individual; not conversations between members of the public.

61. Existing audio-capable cameras that have the potential to capture private conversations must have the audio-capability disconnected, disabled or removed so that it meets the definition of non-audio capable cameras.

62. Programs Branch has assessed sites with existing audio-capable cameras outside of interview rooms to ensure they comply with this standard. The Regions must seek Programs Branch validation on any new installations involving audio-capable cameras.

63. Audio information which is inadvertently captured in a manner inconsistent with this policy cannot be used by the CBSA and must be destroyed. Details of this incident must be sent to Programs Branch via the AV Policy Inbox: CBSA-ASFC_AV_Policy-Politique_AV

Signage

64. Except as provided below, the use of any audio-video monitoring and recording technology by the CBSA in an area owned, operated or controlled by the CBSA **shall be made known** to CBSA employees and the public. Clear and visible signage indicating that an area is under audio-video monitoring or recording by the CBSA, including instructions to ask to speak with a supervisor or visit CBSA's website for more information, must be posted.

65. The specifications for the signage will be in accordance with the Treasury Board's Federal Identity Program requirements.

66. Signage is not required when monitoring or recording technology is used with the knowledge and consent of the person being monitored or recorded.

Storage and Access

Equipment

67. All audio-video recordings shall be securely stored as per CBSA policy on the storage of protected information when they are not in use. Audio-video recordings are classified as "Protected B." (Refer to Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets).

68. The requirement for secure storage applies to any equipment containing recordings, such as: cameras, voice recorders and recording mediums (films, cassettes, discs, memory keys, etc). A record of access to the recordings and equipment shall be kept by way of electronic or manual log.

69. Only those persons who are trained to use the audio-video monitoring and recording equipment will be authorized to have access to or control of such equipment. Authorization must be provided in writing by the manager responsible for the facility in which the equipment is located and must specify the purpose(s) for which access and control is given.

70. For the purposes of this section, control means the ability to move, manipulate or otherwise guide the direction, focus or magnification of a camera by remote means and includes the ability to initiate, stop, reverse or overwrite audio or video recording.

Access to Records

71. It is the policy of the CBSA to limit and restrict access to records made from the use of any audio-video recording technology. Only persons who are authorized and whose work requires it as part of their official or assigned duties will be permitted to have access to records, to view and/or listen to, or make copies of records. This applies equally to records made by third parties and provided to the CBSA for any reason.

72. The following persons are authorized to access, to view and/or to listen to and make copies of records in accordance with paragraph 71, above:

    (a) The President, Executive Vice-President or any Vice President of the CBSA, or any person authorized by the President, Executive Vice-President or any Vice President of the CBSA;
    (b) A director general, director or manager of a headquarters program area, or an official of that program area who is authorized by their manager to have access to or to view records and who requires such access as a part of his or her official duties;
    (c) A regional director general, director or manager of a regional program area or an official of that program area authorized by their manager to have access to or to view records and who requires such access as a part of his or her official duties;
    (d) A director or chief of operations at any CBSA office in which the record is kept, or a superintendent or other official reporting to that chief who is authorized by that chief to have access to or to view records and who requires such access as a part of his or her official duties;
    (e) A regional or headquarters security official who requires such access as a part of his or her official duties;
    (f) The manager or an investigator of the Professional Standards Investigations Section of the Security and Professional Standards Directorate;

73. The following persons may be authorized to have access to and be permitted to view records and may make copies of records in accordance with paragraph 71, above:

    (a) An employee of the CBSA who is authorized to do so by a person listed in paragraph 72;
    (b) An official of a program area working within the mandate of the program and carrying out the duties expected of his/her position who is authorized to do so by a person listed in paragraph 72;
    (c) Any person authorized to have access to or to view or listen to a record in accordance with the provisions of the *Privacy Act*, the *Customs Act*, the *Immigration and Refugee Protection Act* or the *Proceeds of Crime Money Laundering and Terrorist Financing Act*, and the policies of the CBSA in respect of such access and its authorization who is authorized to do so by a person listed in paragraph 72.

Transmission of Audio-Video Data over Wireless Networks

74. All audio-video information transmitted over a wireless network must be transmitted in accordance with established CBSA/CRA protocols on wireless data transmission. Refer to CBSA's Policy on the use of Wireless Technology.

75. Any wireless transmission of audio-video data that is not in compliance with these protocols must cease immediately upon the implementation of this policy. The wireless transmission can only resume when certification from local IT and

authorization from an official of the Physical Security Section of the Security and professional Standards Directorate is received to indicate that the wireless installation is now in compliance with these protocols.

Copying of Records

76. Recordings shall only be copied for uses consistent with the permitted uses of audio-video monitoring and recording technology, as outlined in paragraphs 42 - 52, or to comply with a court order or a direction of a tribunal or board of inquiry to make or provide copies.

77. When copies of recordings are required for evidence, the copy of the audio-video tape, disk, flash drive, hard drive or any other memory device must contain the complete sequence of events.

78. All copies of recordings must be made in duplicate and certified by two CBSA employees to be true copies of the original.

79. Where technology allows, all original recordings should be safeguarded in accordance with the principles of evidence collection and secure storage and with regard for principles of evidence handling.

Retention of Records

80. If a camera is used strictly for live-monitoring purposes, there is no requirement to make recordings, for example in the case of motion- or video analytics-activated cameras for physical security of facilities. If recordings are made, they must be retained in accordance with paragraphs 81 and 83 below.

81. Recordings of any audio-video monitoring activity must be retained for no less than thirty (30) days following the date of their creation.

    Note: This clause does not apply to audio-video technology already in use that is unable to meet this requirement. Any new or replacement audio-video monitoring and recording equipment purchased following the implementation of this policy must be capable of storing data for the minimum retention period.

82. Only those records falling within the definition of transitory records found in paragraph 21 of this policy may be destroyed when they are no longer required and upon the expiry of the minimum retention period outlined in paragraph 81 of this policy.

83. Recordings that are used to obtain or provide information or to investigate an allegation or complaint, or used as evidence in respect of an identifiable individual shall be kept for the longer of two (2) years following the date of their creation, or following the date of their last use in an administrative action as information or as

evidence in respect of that person. These records will be retained and disposed of in accordance with the appropriate Institution Specific Disposition Authority (ISDA).

Recordings made by Third Parties

84. Any and all recordings made by a third party, such as an airport or bridge authority, and provided to the CBSA for any reason must be retained in accordance with paragraph 83.

85. The CBSA has a duty to ensure that the chain of custody of such recordings is maintained for court purposes and must store them securely in accordance with paragraph 67.

86. The CBSA will endeavour to enter into a memorandum of understanding with any authority that has installed cameras in CBSA areas for which the CBSA does not have principal control or use in order to ensure that CBSA information is not disclosed or shared with any third party without the consent of the CBSA.

Disclosure / Information Sharing

87. All disclosure of audio-video records must be made in accordance with the provisions of the *Customs Act*, the *Access to Information Act*, the *Privacy Act* and/or CBSA Disclosure Policy.

88. When an audio-video recording is disclosed in response to an ATIP request from an individual whose information is contained in the record, the identity and other personal information of other individuals in the audio-video recording who are not implicated in the request will be protected. If the personal information of a third party cannot be protected, and consent has not been provided for its disclosure, the audio-video record will not be disclosed.

Disposal of Recordings and Equipment

89. Upon the expiration of the retention period, recordings must be properly disposed of in accordance with CBSA policy. Refer to Comptrollership Manual – Security Volume, Chapter 8: Disposal of Sensitive Information and Assets.

90. Audio-video monitoring and recording equipment must also be disposed of in accordance with Comptrollership Manual – Security Volume, Chapter 8: Disposal of Sensitive Information and Assets.

Standards

91. The CBSA will establish and maintain specifications and technical standards for audio-video monitoring and recording technology equipment and other peripheral equipment. Specifications and technical standards will be based on the intended usage of equipment and on the need for compatibility and interoperability between

CBSA offices. Where a camera or other device serves more than one purpose, the higher standards will apply.

92. Each region is responsible for maintaining an inventory of audio-video monitoring and recording technology equipment and peripheral equipment, including the location where such equipment is installed or stored, the purpose for each camera in use, and the retention capability of the recording system, and must provide information to the Emerging Border Programs Division of the Border Programs Directorate, Programs Branch.

Roles and Responsibilities

93. The Programs Branch (Compliance and Programs Management Division) is responsible for:

    (a) national program development and direction;
    (b) administering and delivering the program to the field
    (c) maintaining and updating the audio-video policy;
    (d) implementation of this policy;
    (e) monitoring compliance with this policy;
    (f) maintaining a national inventory of equipment and the location and purpose for each camera, including the retention capability of each recording system;
    (g) providing functional advice and guidance on the application of this policy;
    (h) interpreting applicable legislation and jurisprudence as they relate to the use of audio-video monitoring or recording technology or to the use, access, release or destruction of records;
    (i) validating sites with audio-capable equipment located outside of interview rooms.

94. The Comptrollership Branch (Contracting and Assets Division) is responsible for:

    (a) providing guidance on CCTV cameras, recording devices and peripheral equipment as it relates to their purchase, acquisition, installation, and maintenance.

95. The Comptrollership Branch (Security and Professional Standards Directorate) is responsible for:

    (a) providing advice and guidance on CCTV cameras, recording devices and peripheral equipment as it relates to security;
    (b) ensuring that security is provided or maintained for inventory and assets including audio-video monitoring or recording technology and any medium;
    (c) conducting Security and Professional Standards Directorate investigations where serious security breaches have occurred or in response to complaints involving questions of conduct or integrity of the CBSA and its officers that are serious enough to involve the Professional Standards Investigations Division of the Security and Professional Standards Directorate.

(d) providing guidance when hiring external contractors to make sure that security and confidentiality are maintained.

96. The Information, Science and Technology Branch (Science and Engineering Directorate) is responsible for the following:

(a) identifying, developing and testing new technology as it relates to audio-video monitoring or recording devices;
(b) developing and maintaining specifications for CCTV cameras, recording devices and peripheral equipment in accordance with this policy.

97. The Operations Branch - Regions is responsible for:

(a) complying with this policy and legislation on the use of audio-video monitoring and recording technology and retention of records;
(b) reporting incidents of tampering, loss or damage to equipment or data;
(c) communicating with headquarters program areas on issues related to equipment, technology and policy;
(d) contacting the Science and Engineering Directorate for installation and / or replacement of new cameras, replacement of new recording systems and installation of new CCTV/AVMS technology;
(e) contacting certified service providers for the regular maintenance and repairs of CCTV/AVMS equipment;
(f) conducting an inventory as per the requirements of paragraph 92 within three (3) months of the implementation of this policy and for providing this information to the Emerging Border Programs Division of the Border Programs Directorate, Programs Branch;
(g) maintaining regional inventory list of equipment, including the location and purpose of each camera, and for providing inventory updates to the Emerging Border Programs Division of the Border Programs Directorate, Programs Branch.

98. The Operations Branch – Headquarters is responsible for:

(a) identifying operational impacts;
(b) supporting the integrity and professional standards strategy;
(c) ensuring that operational concerns raised by Regional Operations are brought forward to the Programs Branch.

99. Employees of the CBSA are responsible for:

(a) complying with this policy;
(b) reporting any misuse of audio-video monitoring or recording technology, unauthorized access to equipment or records or unauthorized listening, viewing, copying or release of records;
(c) completing and submitting a Security Incident Report should theft and/or compromise of audio-video monitoring and recording technologies occur.

(Refer to: Comptrollership Manual – Security Volume – Chapter 15: Security Incident Reporting.)

References

Access to Information Act;
Canada Border Services Agency Act;
Canadian Charter of Rights and Freedoms;
Criminal Code;
Customs Act;
Federal Court Act;
Immigration and Refugee Protection Act;
Library and Archives of Canada Act;
Privacy Act;
CBSA, "D" Memorandum – D1-16-1;
CBSA, Records Retention and Disposition Policy;
CBSA Security Policies;
Government Security Policy (Treasury Board);
Library and Archives Canada – Multi-Institutional Disposition Authorities (MIDAs);
Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities (Office of the Privacy Commissioner).